Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

01 Project Objectives

02 Network Topology & Critical Vulnerabilities

03 Traffic Profile

04 Normal Behaviour

05 Malicious Behaviour

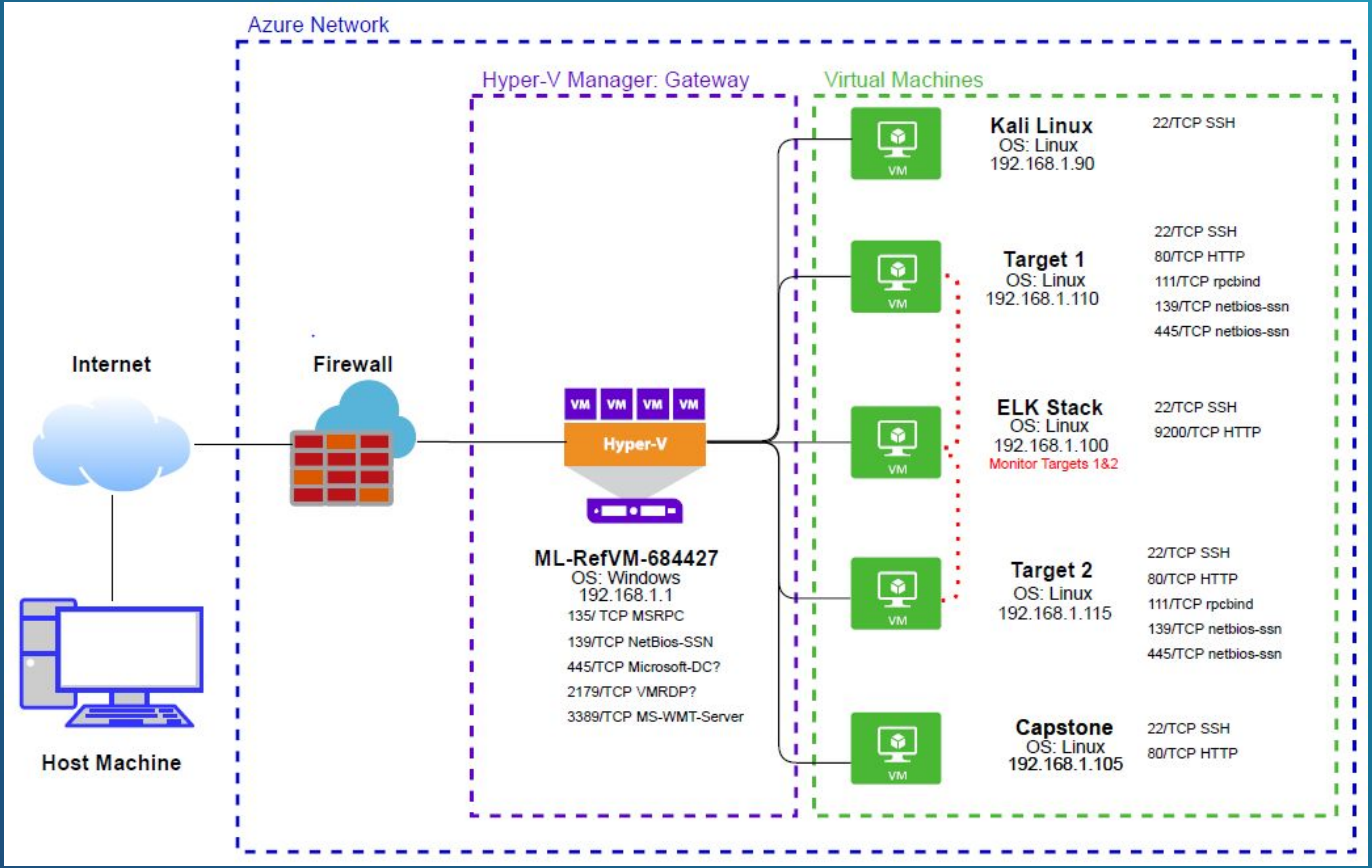
Project Objectives

For our Final Engagement project, our team was tasked with defensive, offensive, and network analysis of a WordPress site. Utilizing an ELK SIEM and Kibana, we set up defensive alerts on our Target VM to monitor for any potential malicious activity. With our Kali VM, we attacked our Target VM to capture 4 flags hidden on the WordPress site and network. Finally, we captured and analyzed network traffic with Wireshark.

Our presentation is focused on the Wireshark network analysis. Once a baseline of normal network traffic was established, our team was able to identify suspicious and malicious activity on the network including illegal torrent downloads and malware.

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.169.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Critical Vulnerabilities: Target 1

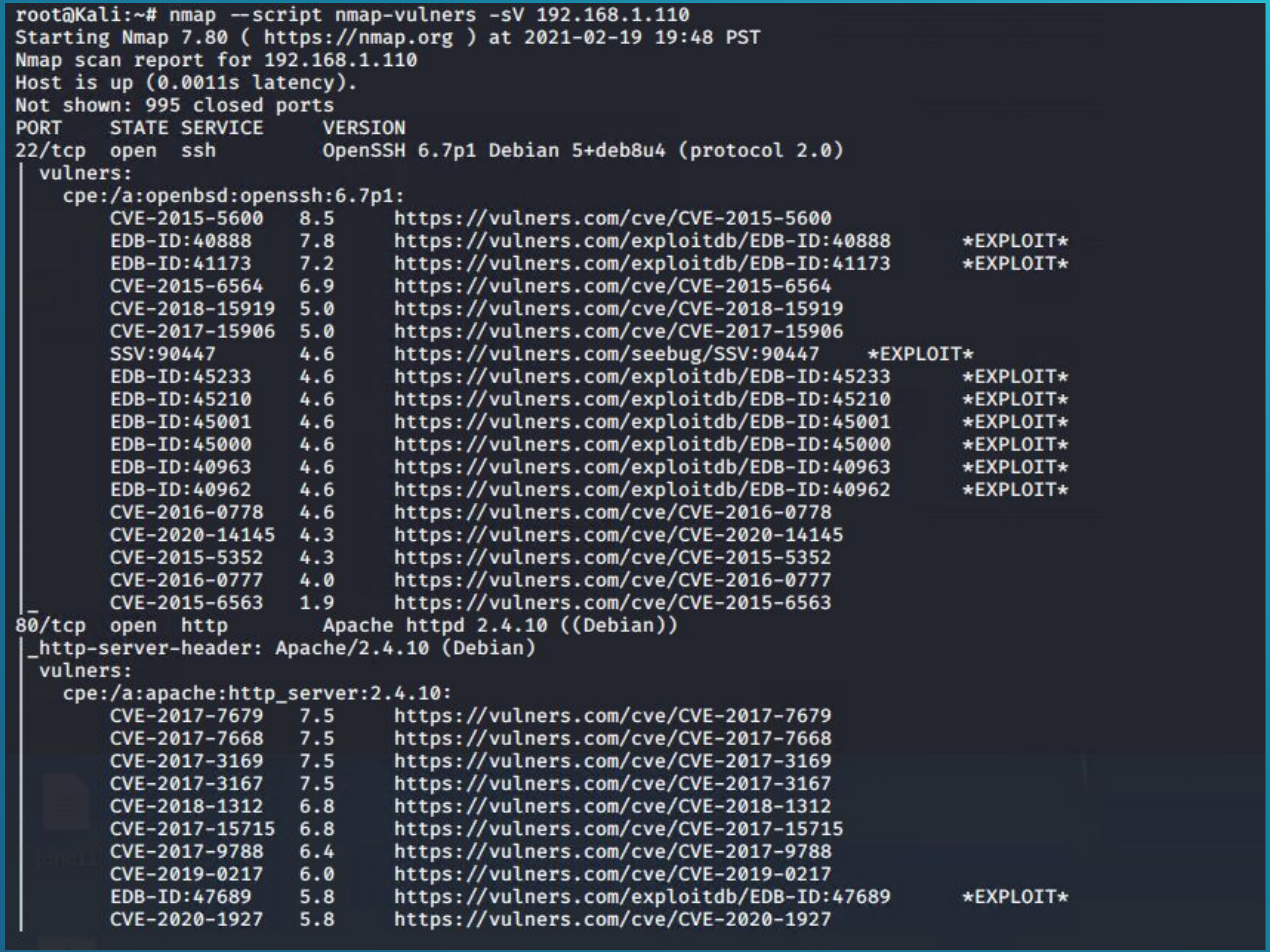
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Severity Level	Description	Impact
CVE-2015-5600	8.5	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection	Remote attackers can bypass security checks on a vulnerable system
CVE-2017-7679	7.5	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	Buffer overflow attack; manipulating the MIME configuration could cause a crash to an httpd child process
CVE-2017-7668	7.5	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string.	Buffer overread attack; With a maliciously crafted HTTP request header, an attacker can potentially cause a segmentation fault

Nmap Vulnerability Scan

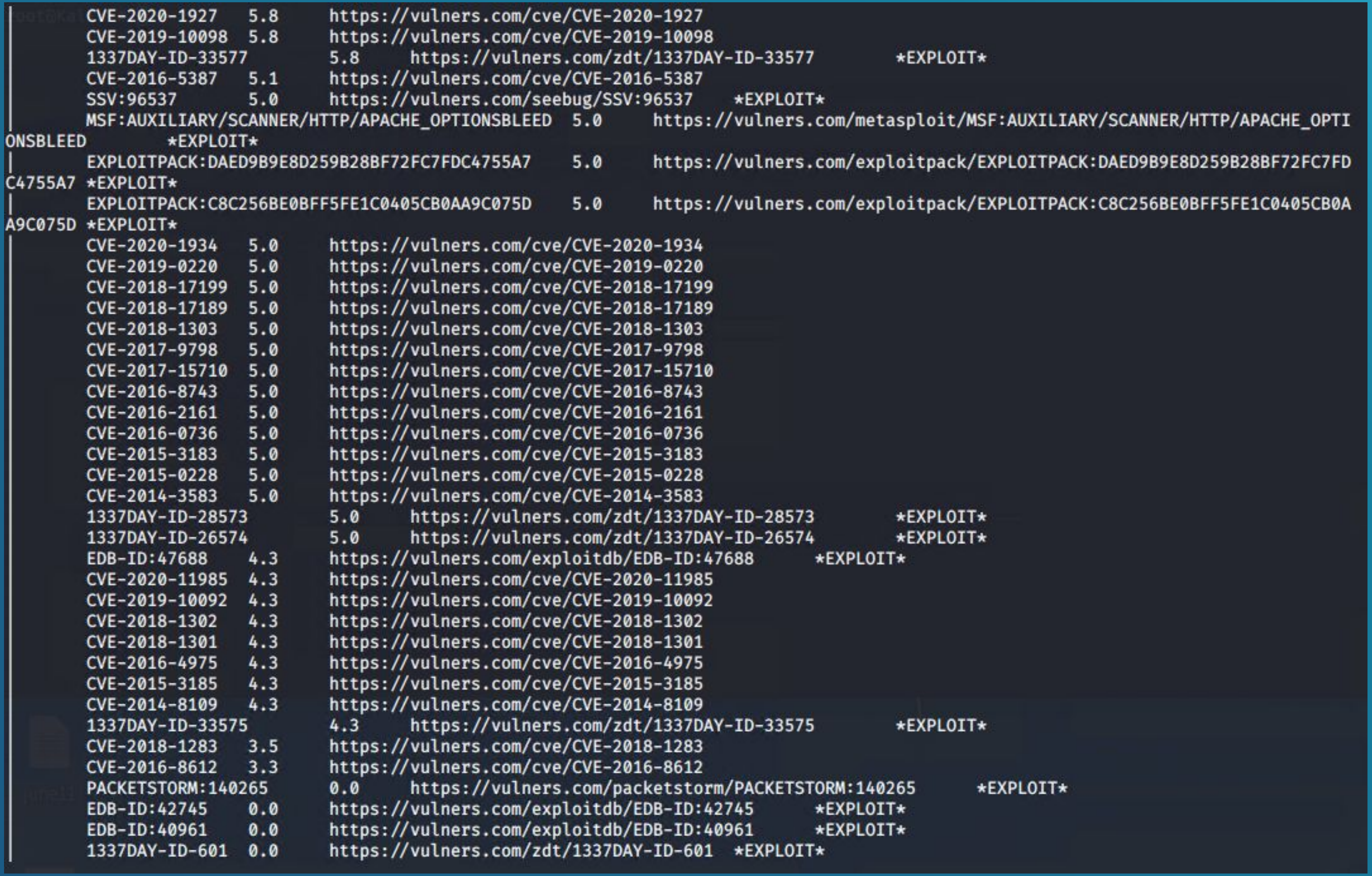
nmap --script vulners -sV 192.168.1.110

Utilizing nmap, we identified several critical and high severity vulnerabilities and exploits on Target 1.



```
root@Kali:~# nmap --script nmap-vulners -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-19 19:48 PST
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3169   7.5     https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CVE-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       EDB-ID:47689    5.8     https://vulners.com/exploitdb/EDB-ID:47689      *EXPLOIT*
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
```

Nmap Vulnerability Scan Continued



```
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       CVE-2016-5387   5.1     https://vulners.com/cve/CVE-2016-5387
|       SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED  5.0     https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTI
ONSBLEED        *EXPLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FD
C4755A7 *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0A
A9C075D *EXPLOIT*
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17189  5.0     https://vulners.com/cve/CVE-2018-17189
|       CVE-2018-1303   5.0     https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-9798   5.0     https://vulners.com/cve/CVE-2017-9798
|       CVE-2017-15710  5.0     https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-8743   5.0     https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-2161   5.0     https://vulners.com/cve/CVE-2016-2161
|       CVE-2016-0736   5.0     https://vulners.com/cve/CVE-2016-0736
|       CVE-2015-3183   5.0     https://vulners.com/cve/CVE-2015-3183
|       CVE-2015-0228   5.0     https://vulners.com/cve/CVE-2015-0228
|       CVE-2014-3583   5.0     https://vulners.com/cve/CVE-2014-3583
|       1337DAY-ID-28573        5.0     https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
|       1337DAY-ID-26574        5.0     https://vulners.com/zdt/1337DAY-ID-26574        *EXPLOIT*
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *EXPLOIT*
|       CVE-2020-11985  4.3     https://vulners.com/cve/CVE-2020-11985
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302   4.3     https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301   4.3     https://vulners.com/cve/CVE-2018-1301
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2015-3185   4.3     https://vulners.com/cve/CVE-2015-3185
|       CVE-2014-8109   4.3     https://vulners.com/cve/CVE-2014-8109
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3     https://vulners.com/cve/CVE-2016-8612
|       PACKETSTORM:140265      0.0     https://vulners.com/packetstorm/PACKETSTORM:140265      *EXPLOIT*
|       EDB-ID:42745    0.0     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       EDB-ID:40961    0.0     https://vulners.com/exploitdb/EDB-ID:40961      *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
```

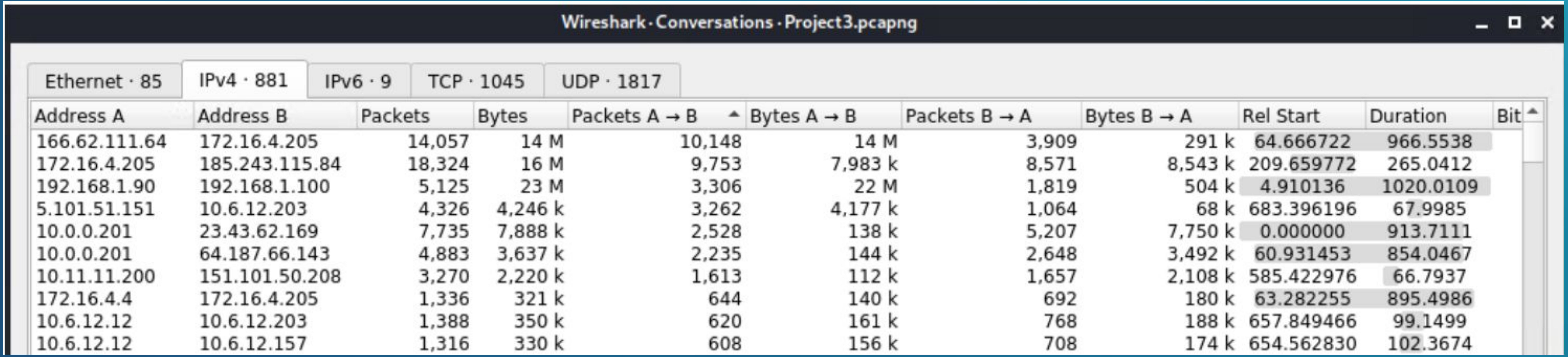
Traffic Profile

3

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

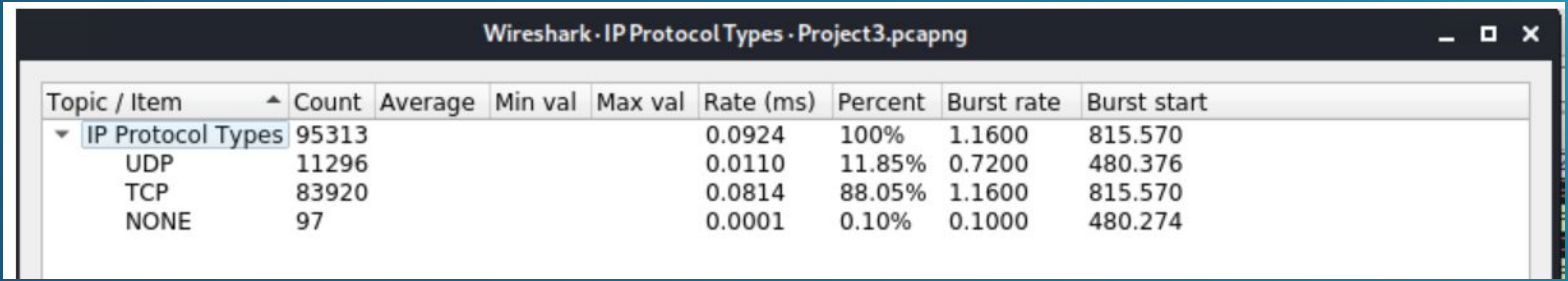
Feature	Value	Description
Top Talkers (IP Addresses)	166.62.111.64- 10,148 packets 172.16.4.205- 9,753 packets 192.168.1.90- 3,306 packets	Top 3 machines that sent the most traffic packets over the network.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bit
166.62.111.64	172.16.4.205	14,057	14 M	10,148	14 M	3,909	291 k	64.666722	966.5538	
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	209.659772	265.0412	
192.168.1.90	192.168.1.100	5,125	23 M	3,306	22 M	1,819	504 k	4.910136	1020.0109	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	683.396196	67.9985	
10.0.0.201	23.43.62.169	7,735	7,888 k	2,528	138 k	5,207	7,750 k	0.000000	913.7111	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	60.931453	854.0467	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	585.422976	66.7937	
172.16.4.4	172.16.4.205	1,336	321 k	644	140 k	692	180 k	63.282255	895.4986	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	657.849466	99.1499	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	654.562830	102.3674	

Traffic Profile Continued

Feature	Value	Description
Most Common Protocols	UDP- 95,313 TCP- 83,920 NONE- 97	The most common protocols with their count on the network.

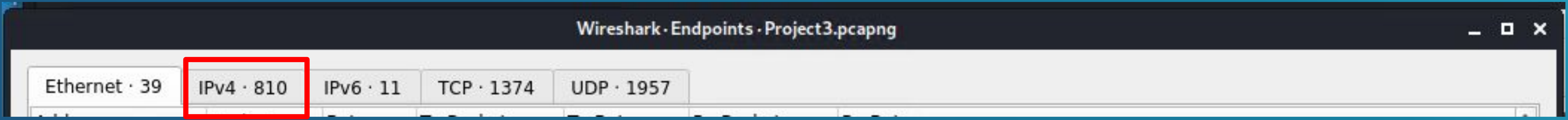


Wireshark · IP Protocol Types · Project3.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Protocol Types	95313				0.0924	100%	1.1600	815.570
UDP	11296				0.0110	11.85%	0.7200	480.376
TCP	83920				0.0814	88.05%	1.1600	815.570
NONE	97				0.0001	0.10%	0.1000	480.274

Traffic Profile Continued

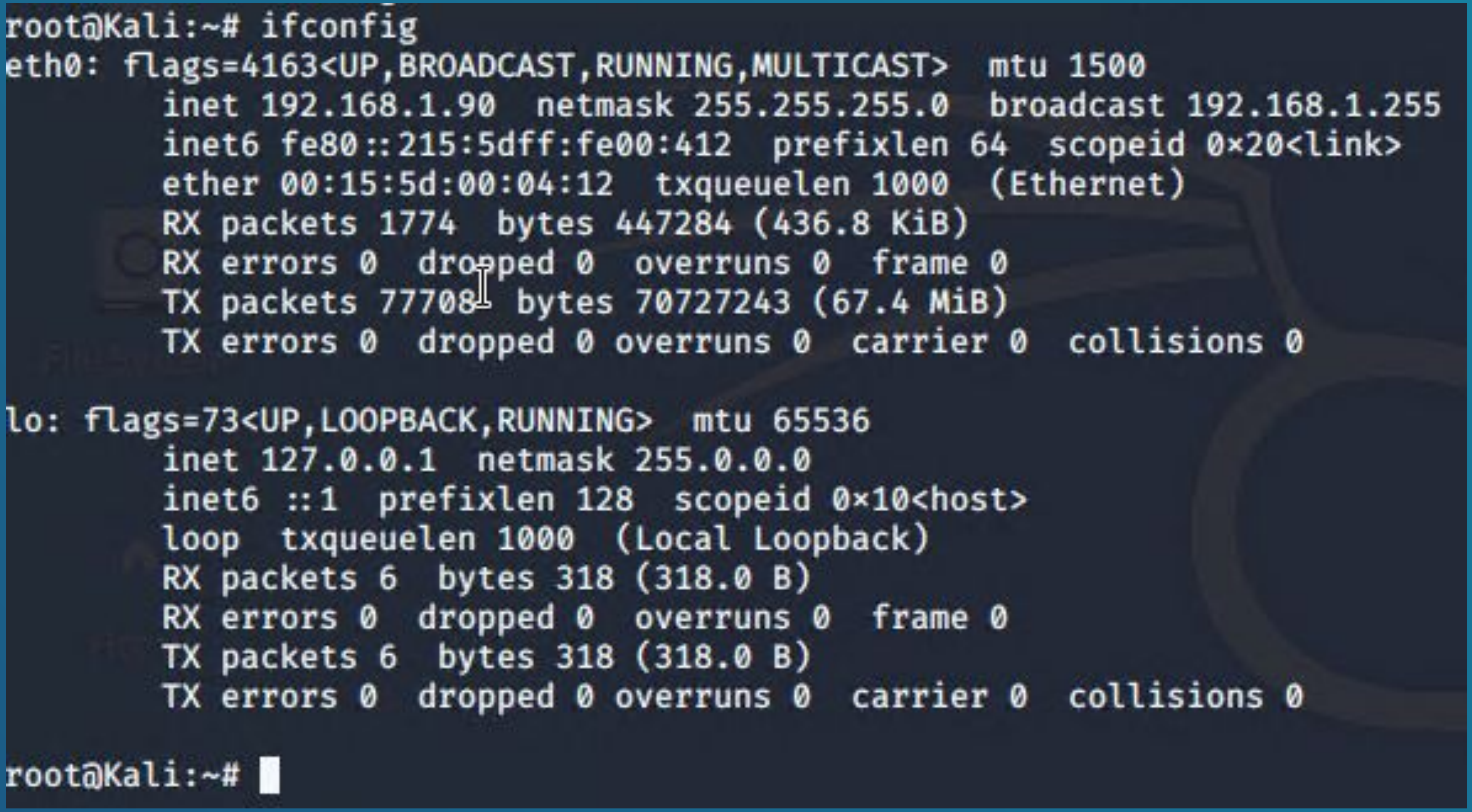
Feature	Value	Description
# of Unique IP Addresses	810 IP address	Count of observed IPv4 addresses.



Wireshark · Endpoints · Project3.pcapng

Traffic Profile Continued

Feature	Value	Description
Subnets	255.255.255.255 255.0.0.0	Observed subnet ranges.



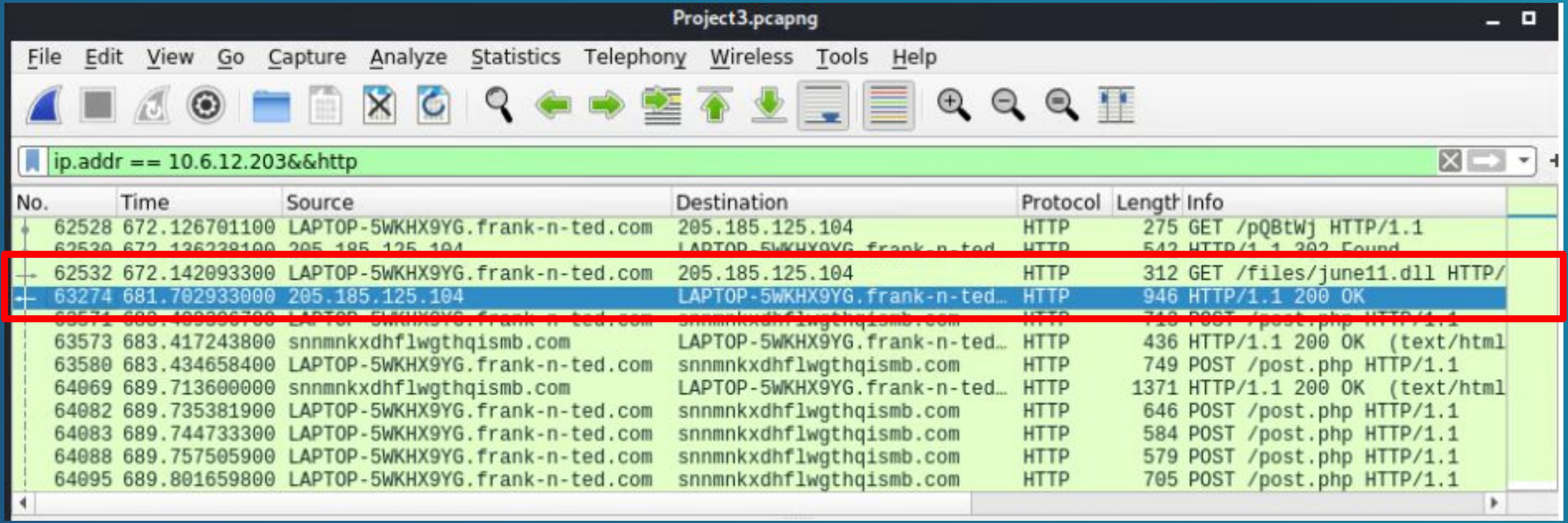
```
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 1774  bytes 447284 (436.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77708  bytes 70727243 (67.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# 
```

Traffic Profile Continued

Feature	Value	Description
# of Malware Species	1 Ransomware Trojan	Number of malware binaries identified in traffic.



Project3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.203&&http

```
No.    Time          Source                               Destination                    Protocol Length Info
 62528 672.126701100 LAPTOP-5WKHX9YG.frank-n-ted.com      205.185.125.104                HTTP      275 GET /pQBtWj HTTP/1.1
 62530 672.136238100 205.185.125.104                      LAPTOP-5WKHX9YG.frank-n-ted…   HTTP      542 HTTP/1.1 302 Found
 62532 672.142093300 LAPTOP-5WKHX9YG.frank-n-ted.com      205.185.125.104                HTTP      312 GET /files/june11.dll HTTP/
 63274 681.702933000 205.185.125.104                      LAPTOP-5WKHX9YG.frank-n-ted…   HTTP      946 HTTP/1.1 200 OK
 63571 683.409396700 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      713 POST /post.php HTTP/1.1
 63573 683.417243800 snnmnkxdhflwgthqismb.com             LAPTOP-5WKHX9YG.frank-n-ted…   HTTP      436 HTTP/1.1 200 OK  (text/html
 63580 683.434658400 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      749 POST /post.php HTTP/1.1
 64069 689.713600000 snnmnkxdhflwgthqismb.com             LAPTOP-5WKHX9YG.frank-n-ted…   HTTP     1371 HTTP/1.1 200 OK  (text/html
 64082 689.735381900 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      646 POST /post.php HTTP/1.1
 64083 689.744733300 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      584 POST /post.php HTTP/1.1
 64088 689.757505900 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      579 POST /post.php HTTP/1.1
 64095 689.801659800 LAPTOP-5WKHX9YG.frank-n-ted.com      snnmnkxdhflwgthqismb.com       HTTP      705 POST /post.php HTTP/1.1
```

Behavioral Analysis

Purpose of Traffic on the Network

Internet browsing

Normal Activity

- Users on the network were confirmed to visit several different sites including:
  - iphonehacks.com searching for different hacks for their iPhone
  - Reading blogs on mysocalledchaos.com
  - Viewing and purchasing vinyl records on vinylmeplease.com

Suspicious Activity

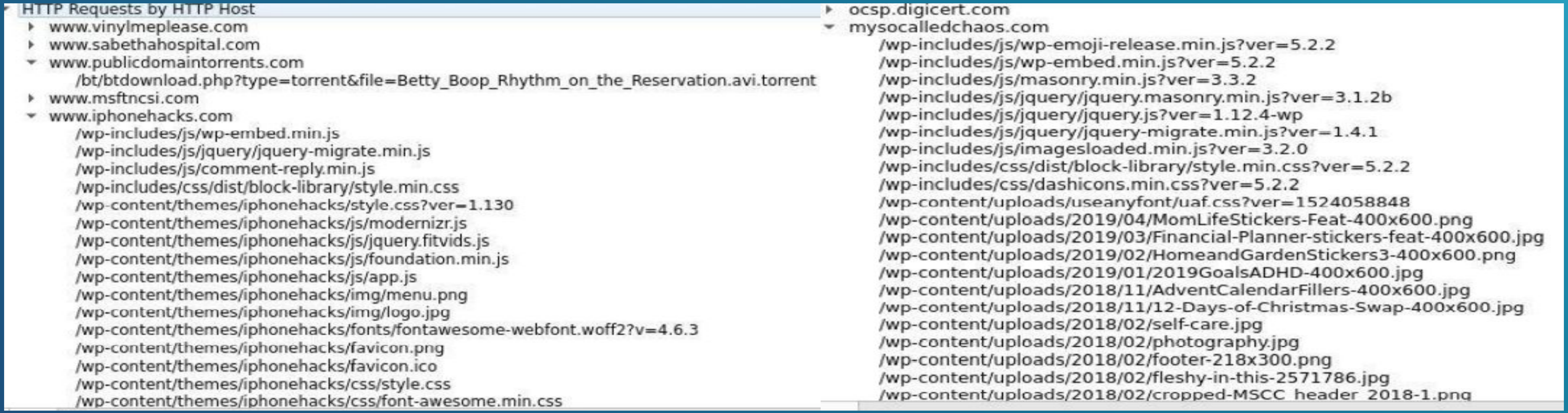
- Large amounts of HTTP and TCP traffic to potentially malicious sites were identified on the network.
  - A user downloaded ransomware Trojan.Mint.Zamg.O.
- Users we identified downloading torrents on the network.

Normal Activity

Normal Internet Behavior

Summarize the following:

- DNS traffic, HTTP, and TCP packets were all located on the network.
- Users were utilizing the company network to access sites such as iphonehacks.com, mysocalledchaos.com, vinylmeplease.com, etc.

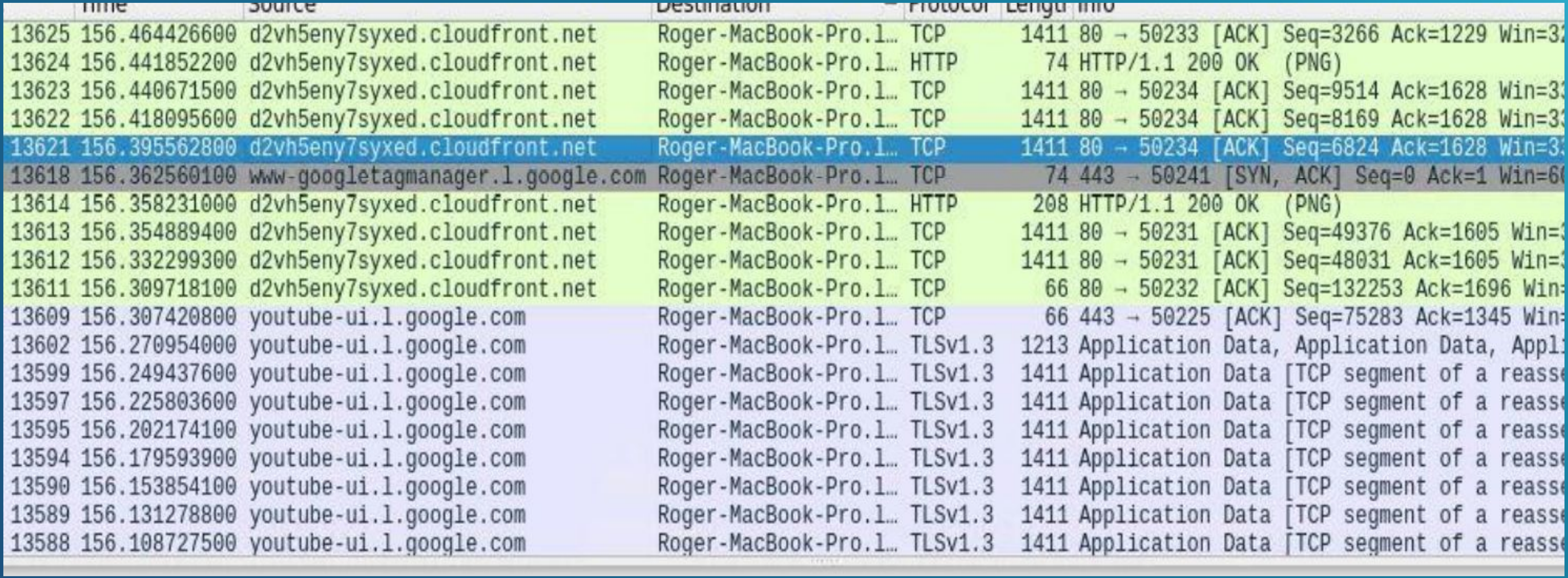


```
HTTP Requests by HTTP Host
  ▸ www.vinylmeplease.com
  ▸ www.sabethahospital.com
  ▾ www.publicdomaintorrents.com
      /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
  ▸ www.msftncsi.com
  ▾ www.iphonehacks.com
      /wp-includes/js/wp-embed.min.js
      /wp-includes/js/jquery/jquery-migrate.min.js
      /wp-includes/js/comment-reply.min.js
      /wp-includes/css/dist/block-library/style.min.css
      /wp-content/themes/iphonehacks/style.css?ver=1.130
      /wp-content/themes/iphonehacks/js/modernizr.js
      /wp-content/themes/iphonehacks/js/jquery.fitvids.js
      /wp-content/themes/iphonehacks/js/foundation.min.js
      /wp-content/themes/iphonehacks/js/app.js
      /wp-content/themes/iphonehacks/img/menu.png
      /wp-content/themes/iphonehacks/img/logo.jpg
      /wp-content/themes/iphonehacks/fonts/fontawesome-webfont.woff2?v=4.6.3
      /wp-content/themes/iphonehacks/favicon.png
      /wp-content/themes/iphonehacks/favicon.ico
      /wp-content/themes/iphonehacks/css/style.css
      /wp-content/themes/iphonehacks/css/font-awesome.min.css
```

```
  ▸ ocsp.digicert.com
  ▾ mysocalledchaos.com
      /wp-includes/js/wp-emoji-release.min.js?ver=5.2.2
      /wp-includes/js/wp-embed.min.js?ver=5.2.2
      /wp-includes/js/masonry.min.js?ver=3.3.2
      /wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b
      /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
      /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
      /wp-includes/js/imagesloaded.min.js?ver=3.2.0
      /wp-includes/css/dist/block-library/style.min.css?ver=5.2.2
      /wp-includes/css/dashicons.min.css?ver=5.2.2
      /wp-content/uploads/useanyfont/uaf.css?ver=1524058848
      /wp-content/uploads/2019/04/MomLifeStickers-Feat-400x600.png
      /wp-content/uploads/2019/03/Financial-Planner-stickers-feat-400x600.jpg
      /wp-content/uploads/2019/02/HomeandGardenStickers3-400x600.png
      /wp-content/uploads/2019/01/2019GoalsADHD-400x600.jpg
      /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg
      /wp-content/uploads/2018/11/12-Days-of-Christmas-Swap-400x600.jpg
      /wp-content/uploads/2018/02/self-care.jpg
      /wp-content/uploads/2018/02/photography.jpg
      /wp-content/uploads/2018/02/footer-218x300.png
      /wp-content/uploads/2018/02/fleshy-in-this-2571786.jpg
      /wp-content/uploads/2018/02/cropped-MSCC_header_2018-1.png
```

Normal Internet Behavior Continued

- User browsed cloudfront.net and youtube.com.

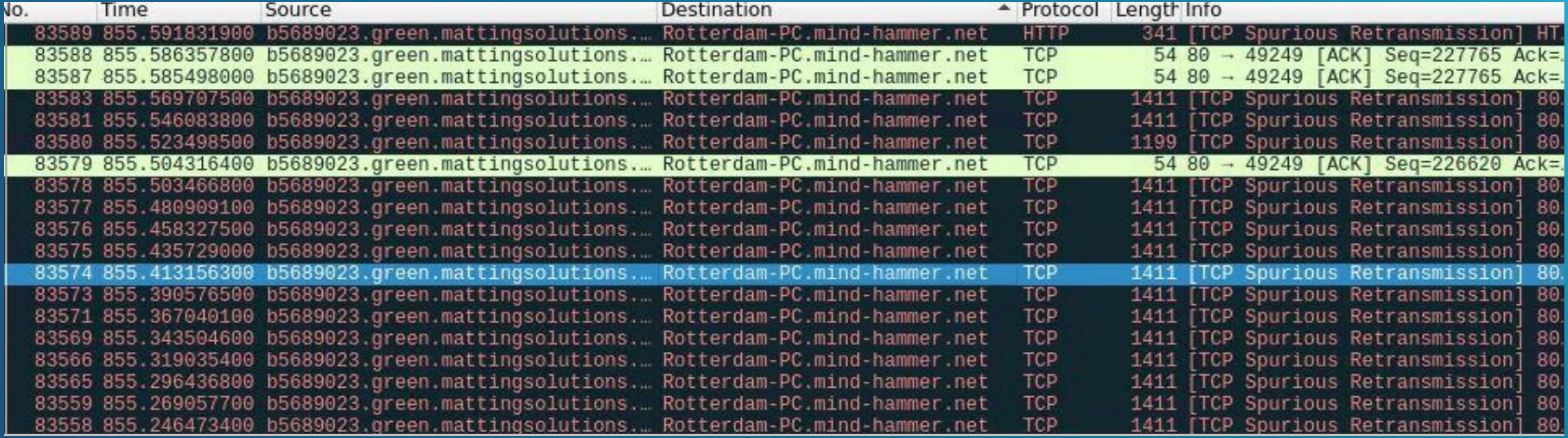


```
      Time        Source                          Destination          Protocol  Length Info
13625 156.464426600 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50233 [ACK] Seq=3266 Ack=1229 Win=32
13624 156.441852200 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… HTTP        74 HTTP/1.1 200 OK  (PNG)
13623 156.440671500 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50234 [ACK] Seq=9514 Ack=1628 Win=3
13622 156.418095600 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50234 [ACK] Seq=8169 Ack=1628 Win=3
13621 156.395562800 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50234 [ACK] Seq=6824 Ack=1628 Win=3
13618 156.362560100 www-googletagmanager.l.google.com Roger-MacBook-Pro.l… TCP       74 443 → 50241 [SYN, ACK] Seq=0 Ack=1 Win=6
13614 156.358231000 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… HTTP       208 HTTP/1.1 200 OK  (PNG)
13613 156.354889400 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50231 [ACK] Seq=49376 Ack=1605 Win=
13612 156.332299300 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP       1411 80 → 50231 [ACK] Seq=48031 Ack=1605 Win=
13611 156.309718100 d2vh5eny7syxed.cloudfront.net   Roger-MacBook-Pro.l… TCP         66 80 → 50232 [ACK] Seq=132253 Ack=1696 Win
13609 156.307420800 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TCP         66 443 → 50225 [ACK] Seq=75283 Ack=1345 Win
13602 156.270954000 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1213 Application Data, Application Data, Appli
13599 156.249437600 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13597 156.225803600 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13595 156.202174100 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13594 156.179593900 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13590 156.153854100 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13589 156.131278800 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
13588 156.108727500 youtube-ui.l.google.com         Roger-MacBook-Pro.l… TLSv1.3   1411 Application Data [TCP segment of a reass
```

Malicious Activity

TCP Spurious Retransmission

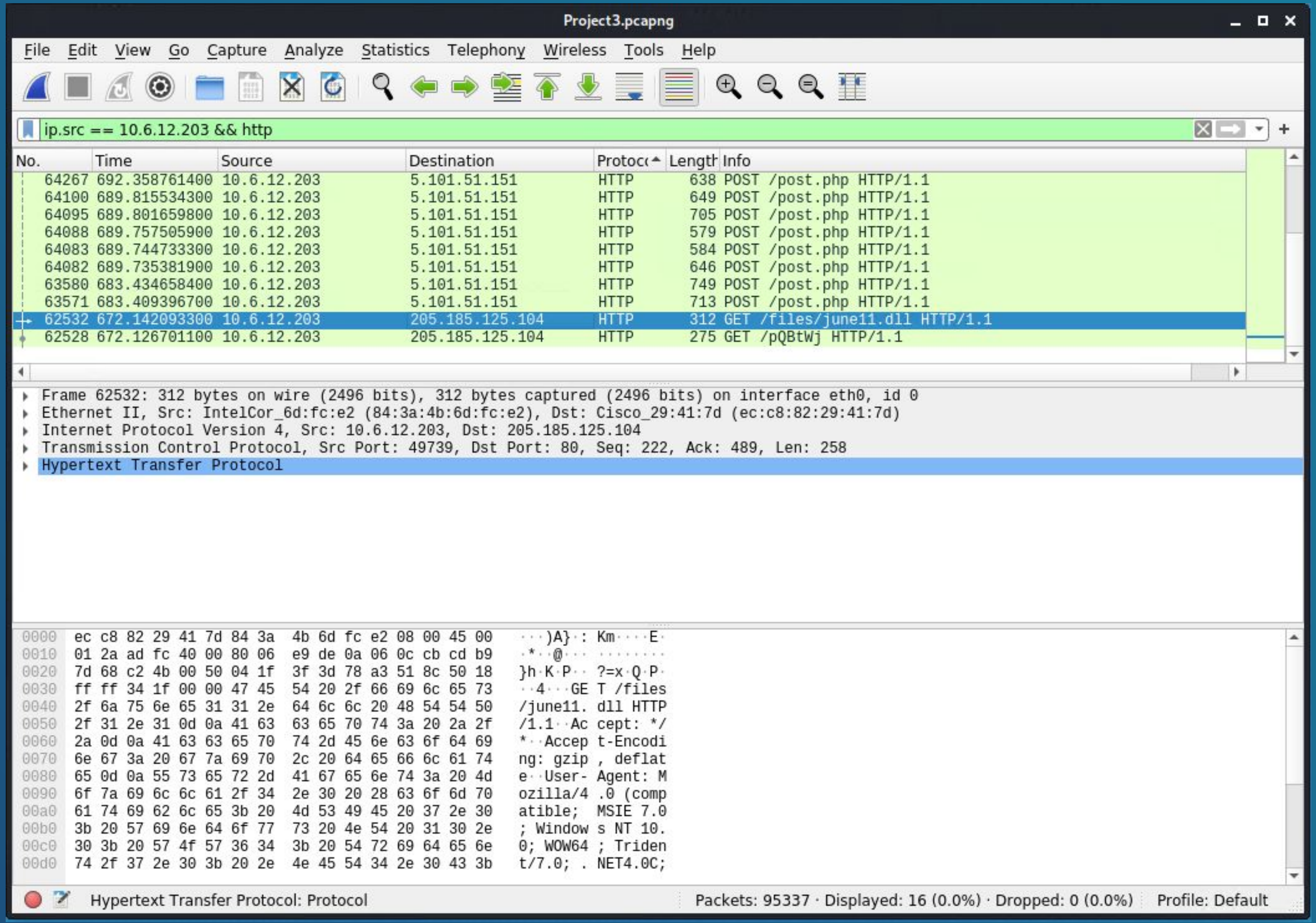
- Large amounts of HTTP and TCP traffic were identified on the network to *.green.mattingsolutions.co site by user matthijs.devries on their Rotterdam-PC.
- A download of a malicious payload on the user's system initiated communication with the attacker site.



No.	Time	Source	Destination	Protocol	Length	Info
83589	855.591831900	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	HTTP	341	[TCP Spurious Retransmission] HT
83588	855.586357800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=227765 Ack=
83587	855.585498000	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=227765 Ack=
83583	855.569707500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83581	855.546083800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83580	855.523498500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1199	[TCP Spurious Retransmission] 80
83579	855.504316400	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=226620 Ack=
83578	855.503466800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83577	855.480909100	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83576	855.458327500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83575	855.435729000	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83574	855.413156300	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83573	855.390576500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83571	855.367040100	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83569	855.343504600	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83566	855.319035400	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83565	855.296436800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83559	855.269057700	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80
83558	855.246473400	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80

Download of Ransomware Trojan

- User matthijs.devries downloaded a ransomware trojan malware from a malicious site.


Project3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

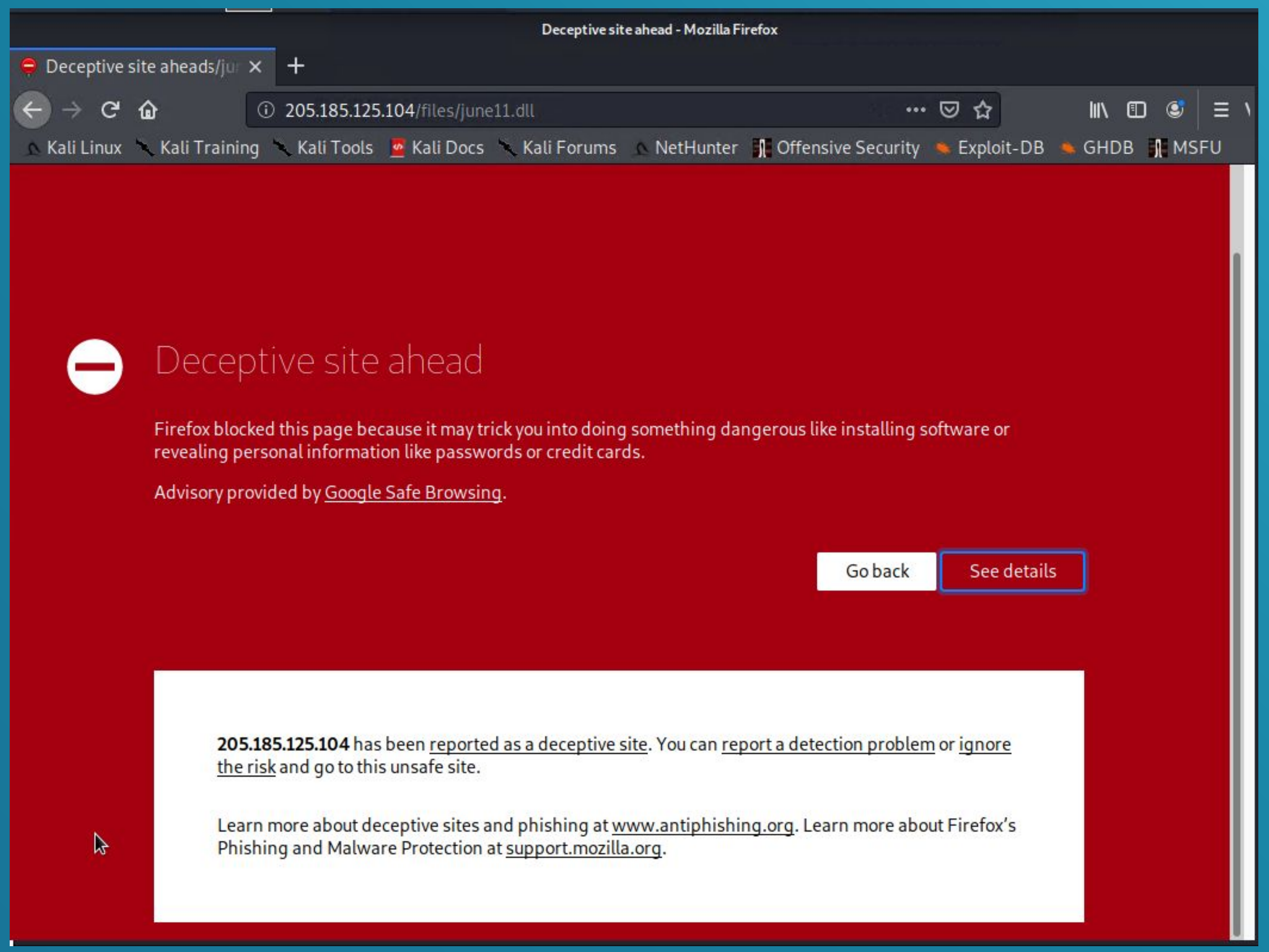
```
ip.src == 10.6.12.203 && http
```

```
No.    Time          Source        Destination     Protocol Length Info
64267 692.358761400 10.6.12.203   5.101.51.151    HTTP      638 POST /post.php HTTP/1.1
64100 689.815534300 10.6.12.203   5.101.51.151    HTTP      649 POST /post.php HTTP/1.1
64095 689.801659800 10.6.12.203   5.101.51.151    HTTP      705 POST /post.php HTTP/1.1
64088 689.757505900 10.6.12.203   5.101.51.151    HTTP      579 POST /post.php HTTP/1.1
64083 689.744733300 10.6.12.203   5.101.51.151    HTTP      584 POST /post.php HTTP/1.1
64082 689.735381900 10.6.12.203   5.101.51.151    HTTP      646 POST /post.php HTTP/1.1
63580 683.434658400 10.6.12.203   5.101.51.151    HTTP      749 POST /post.php HTTP/1.1
63571 683.409396700 10.6.12.203   5.101.51.151    HTTP      713 POST /post.php HTTP/1.1
62532 672.142093300 10.6.12.203   205.185.125.104 HTTP      312 GET /files/june11.dll HTTP/1.1
62528 672.126701100 10.6.12.203   205.185.125.104 HTTP      275 GET /pQBtWj HTTP/1.1
```

```
Frame 62532: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
Hypertext Transfer Protocol
```

```
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
0010  01 2a ad fc 40 00 80 06  e9 de 0a 06 0c cb cd b9   ·*··@··· ········
0020  7d 68 c2 4b 00 50 04 1f  3f 3d 78 a3 51 8c 50 18   }h·K·P·· ?=x·Q·P·
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10.
00c0  30 3b 20 57 4f 57 36 34  3b 20 54 72 69 64 65 6e   0; WOW64 ; Triden
00d0  74 2f 37 2e 30 3b 20 2e  4e 45 54 34 2e 30 43 3b   t/7.0; . NET4.0C;
```

Hypertext Transfer Protocol: Protocol | Packets: 95337 · Displayed: 16 (0.0%) · Dropped: 0 (0.0%) | Profile: Default



Deceptive site ahead

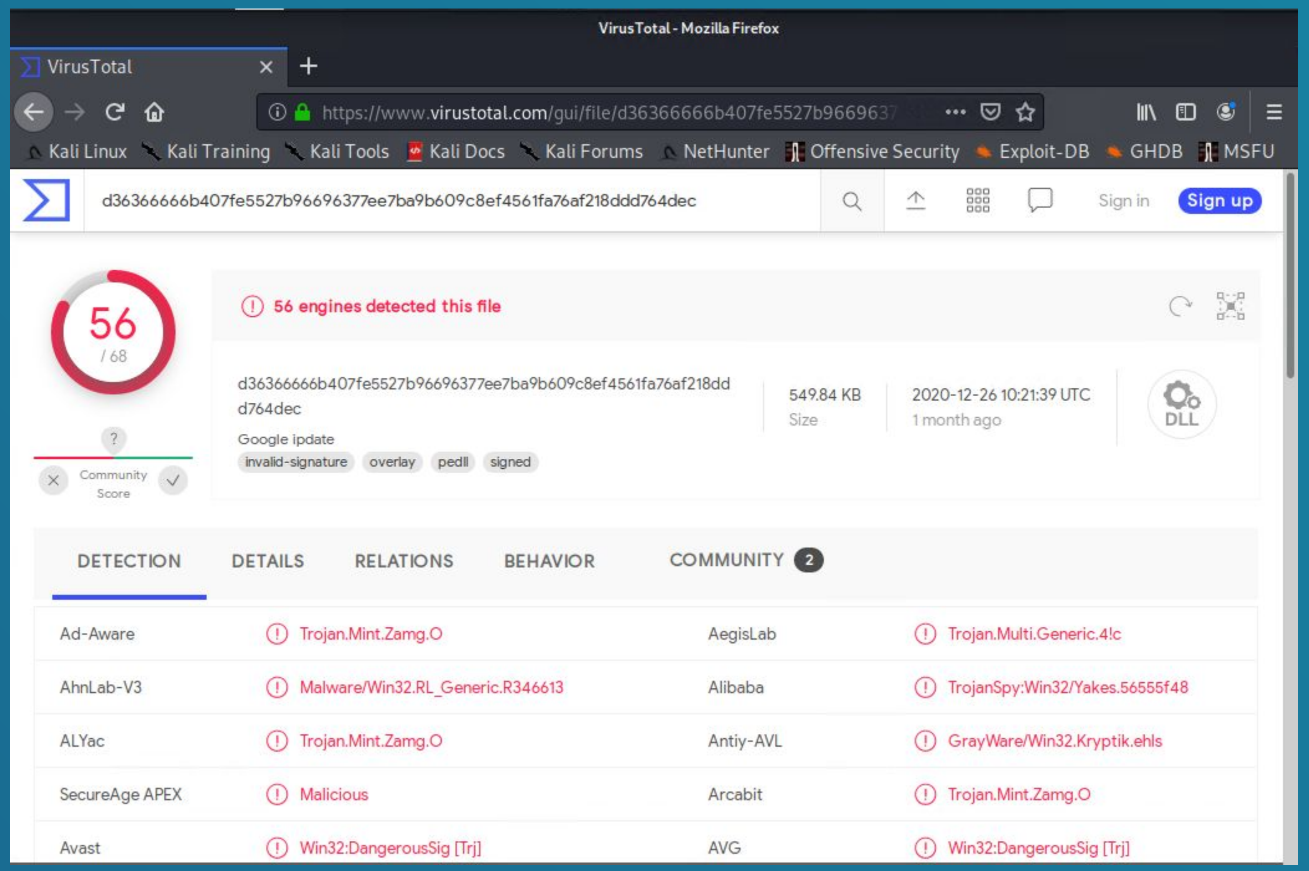
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.

Go back | See details

205.185.125.104 has been reported as a deceptive site. You can report a detection problem or ignore the risk and go to this unsafe site.

Learn more about deceptive sites and phishing at www.antiphishing.org. Learn more about Firefox's Phishing and Malware Protection at support.mozilla.org.



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

56 / 68

56 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google ipdate

invalid-signature overlay pedll signed

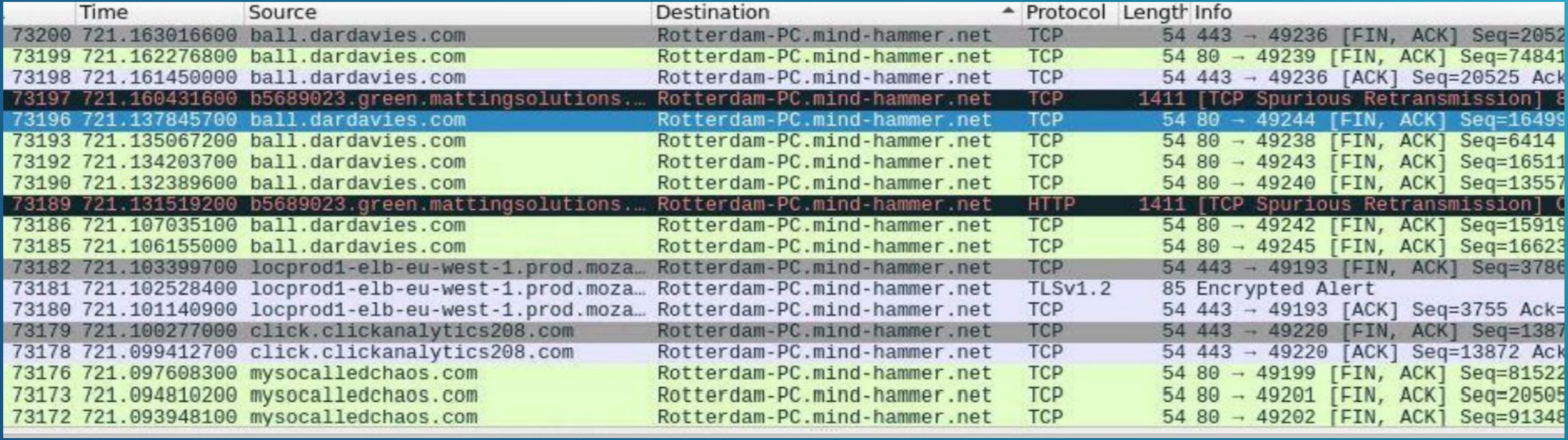
549.84 KB
Size

2020-12-26 10:21:39 UTC
1 month ago

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

Online Sandboxing

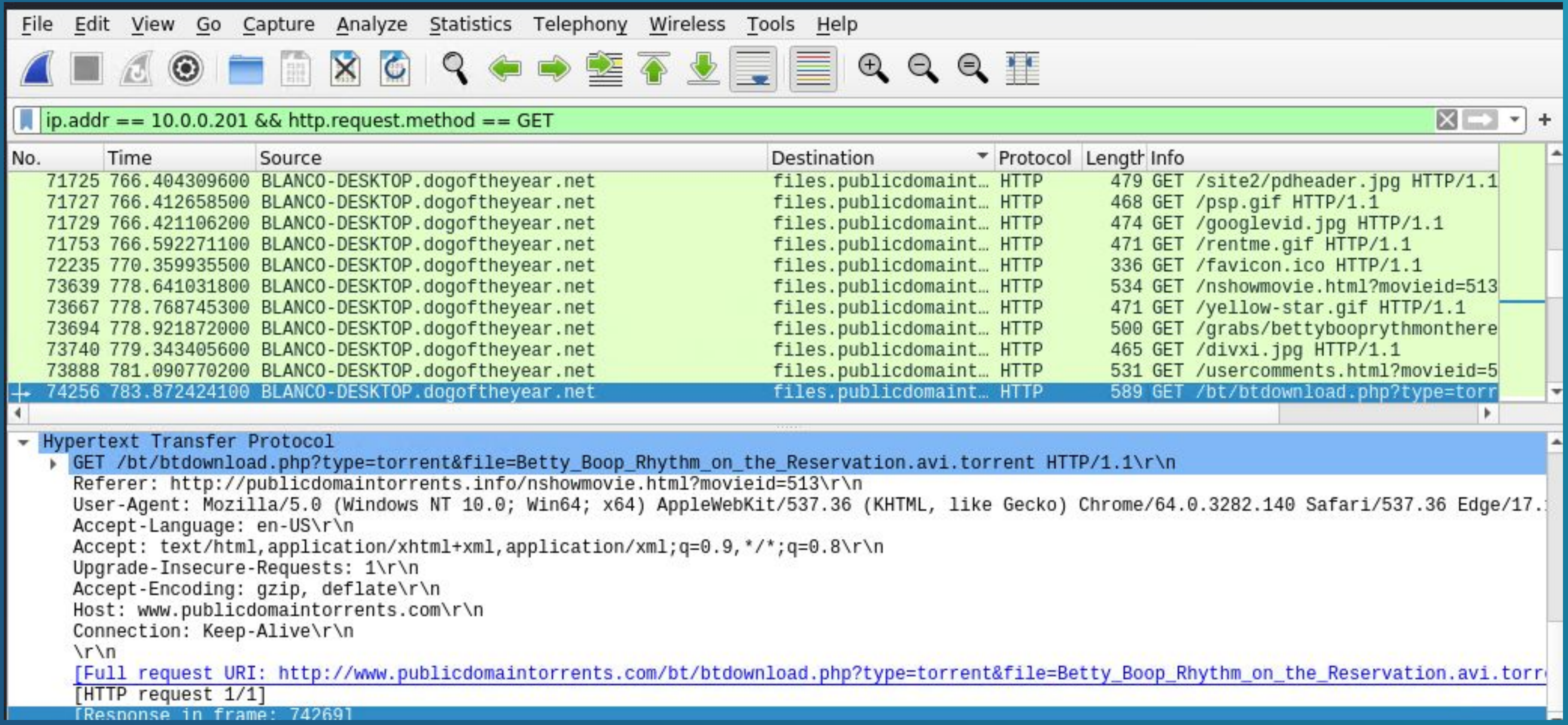
Once the trojan was infecting the system, the user was trying to sandbox the infected files with ball.dardavies.com. While this was occurring, the user was conducting normal internet behavior by visiting mysocalledchaos.com.



	Time	Source	Destination	Protocol	Length	Info
73200	721.163016600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49236 [FIN, ACK] Seq=2052
73199	721.162276800	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49239 [FIN, ACK] Seq=74841
73198	721.161450000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49236 [ACK] Seq=20525 Ack
73197	721.160431600	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 8
73196	721.137845700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49244 [FIN, ACK] Seq=16499
73193	721.135067200	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49238 [FIN, ACK] Seq=6414
73192	721.134203700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49243 [FIN, ACK] Seq=16511
73190	721.132389600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49240 [FIN, ACK] Seq=13557
73189	721.131519200	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	HTTP	1411	[TCP Spurious Retransmission] C
73186	721.107035100	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49242 [FIN, ACK] Seq=15919
73185	721.106155000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49245 [FIN, ACK] Seq=16623
73182	721.103399700	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49193 [FIN, ACK] Seq=3786
73181	721.102528400	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TLSv1.2	85	Encrypted Alert
73180	721.101140900	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49193 [ACK] Seq=3755 Ack=
73179	721.100277000	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49220 [FIN, ACK] Seq=1387
73178	721.099412700	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49220 [ACK] Seq=13872 Ack
73176	721.097608300	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49199 [FIN, ACK] Seq=81522
73173	721.094810200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49201 [FIN, ACK] Seq=20505
73172	721.093948100	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49202 [FIN, ACK] Seq=91348

Torrent Download

User elmer.blanco utilized the company network to download a torrent of the Betty Boop Rhythm on the Reservation movie from publicdomaintorrents.com. While the movie is in the public domain, downloading an unknown torrent file places the network at risk for malware.



ip.addr == 10.0.0.201 && http.request.method == GET

```
No.     Time          Source                        Destination            Protocol Length Info
  71725 766.404309600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      479 GET /site2/pdheader.jpg HTTP/1.1
  71727 766.412658500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      468 GET /psp.gif HTTP/1.1
  71729 766.421106200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      474 GET /googlevid.jpg HTTP/1.1
  71753 766.592271100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      471 GET /rentme.gif HTTP/1.1
  72235 770.359935500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      336 GET /favicon.ico HTTP/1.1
  73639 778.641031800 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      534 GET /nshowmovie.html?movieid=513
  73667 778.768745300 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      471 GET /yellow-star.gif HTTP/1.1
  73694 778.921872000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      500 GET /grabs/bettybooprythmonthere
  73740 779.343405600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      465 GET /divxi.jpg HTTP/1.1
  73888 781.090770200 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      531 GET /usercomments.html?movieid=5
  74256 783.872424100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP      589 GET /bt/btdownload.php?type=torr
```

```
Hypertext Transfer Protocol
  GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
  Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.
  Accept-Language: en-US\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: www.publicdomaintorrents.com\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torr
  [HTTP request 1/1]
  [Response in frame: 74269]
```

References

https://access.redhat.com/security/cve/cve-2015-5600

https://access.redhat.com/security/cve/cve-2017-7679

https://access.redhat.com/security/cve/CVE-2017-7668

https://vulners.com/cve/CVE-2015-5600

https://vulners.com/cve/CVE-2017-7679

https://vulners.com/cve/CVE-2017-7668

https://www.virustotal.com/gui/

The End